Data protection

A practical guide to IT security

Ideal for the small business

ico.
Information Commissioner's Office

Under the Data Protection Act, you have responsibilities to protect the personal information that you and your staff collect and use. This includes a requirement to have appropriate security to prevent it being accidentally or deliberately compromised.

Breaches of data protection legislation could lead to your business incurring a fine – up to £500,000 in serious cases. The reputation of your business could also be damaged if inadequate security contributes to high profile incidents of data loss or theft.

This guide gives advice for small businesses on how to keep IT systems safe and secure.

10 practical ways to keep your IT systems safe and secure

Keeping your IT systems safe and secure can be a complex task and does require time, resource and specialist knowledge. If you have personal data within your IT system you need to recognise that it may be at risk and take appropriate technical measures to secure it. The measures you put in place should fit the needs of your particular business. They don't necessarily have to be expensive or onerous. They may even be free or already available within the IT systems you currently have.

The following practical steps will help you decide how to manage the security of the personal data you hold.

1 Assess the threats and risks to your business

Before you can establish what level of security is right for your business you will need to review the personal data you hold and assess the risks to that data. You should consider all processes involved that require you to collect, store, use and dispose of personal data.

Consider how valuable, sensitive or confidential the information is and what damage or distress could be caused to individuals if there was a security breach.

With a clear view of the risks you can begin to choose the security measures that are appropriate for your needs. The next step is to begin putting them in place.

Get in line with Cyber Essentials

2

What is the problem?

There is no single product that will provide a complete guarantee of security for your business. The recommended approach is to use a set of security controls that complement each other but will require ongoing support in order to maintain an appropriate level of security.

What can I do?

The UK Government's Cyber Essentials Scheme describes the following five key controls for keeping information secure. Obtaining a Cyber Essentials certificate can provide certain security assurances and help protect personal data in your IT systems.

Boundary firewalls and internet gateways

This will be your first line of defence against an intrusion from the internet. A well configured firewall can stop breaches happening before they penetrate deep into your network. An internet gateway can prevent users within your organisation accessing websites or other online services that present a threat or that you do not trust.

2

Secure configuration

Almost all hardware and software will require some level of set-up and configuration in order to provide the most effective protection. You should remove unused software and services from your devices to reduce the number of potential vulnerabilities. Older versions of some widespread software have well documented security vulnerabilities. If you don't use it, then it is much easier to remove it than try to keep it up-to-date.

Make sure you have changed any default passwords used by software or hardware – these are well known by attackers.

Access control

Restrict access to your system to users and sources you trust. Each user must have and use their own username and password.

Each user should use an account that has permissions appropriate to the job they are carrying out at the time. You should also only use administrator accounts when strictly necessary (eg for installing known and trusted software).

A brute force password attack is a common method of attack, perhaps even by casual users trying to access your Wi-Fi so you need to enforce strong passwords, limit the number of failed login attempts and enforce regular password changes.

Passwords or other access should be cancelled immediately if a staff member leaves the organisation or is absent for long periods.

2

Malware protection

You should have anti-virus or anti-malware products regularly scanning your network to prevent or detect threats. You will also need to make sure they are kept up-to-date and that it is switched on and monitoring the files that it should be. You should also make sure you receive and act upon any alerts issued by the malware protection.

Patch management and software updates

Computer equipment and software need regular maintenance to keep it running smoothly and to fix any security vulnerabilities. Security software such as anti-virus and anti-malware needs regular updates in order to continue to provide adequate protection.

Keep your software up-to-date by checking regularly for updates and applying them. Most software can be set to update automatically.

If your system is a few years old, you should review the protection you have in place to make sure that it is still adequate.

3 Secure your data on the move and in the office

What is the problem?

The physical security of equipment is important to consider as devices containing personal data could be stolen in a break-in or lost whilst away from the office. You should ensure that personal data on your systems is protected against these types of threats.

You can also prevent or limit the severity of data breaches by separating or limiting access between your network components. For example, if you can confine the processing of personal data to a specific section of your network you may be able to reduce the scope of the required security measures.

You also need to ensure that the same level of security is applied to personal data on devices being used away from the office. Many data breaches arise from the theft or loss of a device (eg laptop, mobile phone or USB drive) but you should also consider the security surrounding any data you send by email or post.

Allowing untrusted devices to connect to your network or using work devices on untrusted networks outside your office can also put personal data at risk.

What can I do?

You can increase the physical security of your office including storing your servers in a separate room with added protection. Back-up devices, CDs and USBs should not be left unattended and should be locked away when not in use.

You can ensure that personal data is either not on the device in the first place or that it has been appropriately secured so that it cannot be accessed in the event

of loss or theft. Good access control systems and encryption will help here.

Encryption is a means of ensuring that data can only be accessed by authorised users. Typically, a (strong) password is required to 'unlock' the data. You can find more information on choosing the right encryption on our website.

Encryption comes in many different forms and offers protection under different circumstances.

- Full disk encryption means that all the data on the computer is encrypted.
- File encryption means that individual files can be encrypted.
- Some software offers password protection to stop people making changes to the data but this may not stop a thief reading the data. Make sure you know exactly what protection you are applying to your data.

Some mobile devices support a remote disable or wipe facility. This allows you to send a signal to a lost or stolen device to locate it and, if necessary, securely delete all data. Your devices will normally need to be pre-registered to use a service like this.

If you permit employees or other users to connect their own devices to your network you will be increasing the range of security risks and these should also be addressed. You can find more information about these risks in the ICO's guidance on Bring Your Own Device (BYOD).

4 Secure your data in the cloud

What is the problem?

There are a wide range of online services, many incorporated within today's smartphones and tablets that require users to transfer data to remote computing facilities – commonly known as the cloud.

Processing data in the cloud represents a risk because the personal data for which you are responsible will leave your network and be processed in those systems managed by your cloud provider. You therefore need to assess the security measures that the cloud provider has in place to ensure that they are appropriate.

What can I do?

Make sure you know what data is being stored in the cloud as modern computing devices, especially those targeted at consumers, can have cloud backup or sync services switched on by default.

Consider the use of two factor authentication especially for remote access to your data in the cloud.

You can find more information about the use of cloud services in the ICO's Guidance on the use of cloud computing.

Back up your data

5

What is the problem?

If you were to suffer a disaster such as fire, flood or theft you need to be able to get back up and running as quickly as possible. Loss of data is also a breach of the DPA.

Malware can also disrupt the availability of access to your data. Known as 'ransomware' this type of malware can encrypt all your data and only provide you with the means to decrypt the data after payment of a ransom.

What can I do?

You need to have a robust data backup strategy in place to protect against disasters but also malware, such as ransomware.

Back-ups should not be stored in a way that makes them permanently visible to the rest of the network. If they are then they can be encrypted by malware or the files accidentally deleted.

At least one of your back-ups should be off-site.

6 Train your staff

What is the problem?

Your employees may have a limited knowledge of cyber security but they could be your final line of defence against an attack. Accidental disclosure or human error is also a leading cause of breaches of personal data. This can be caused by simply sending an email to the incorrect recipient or opening an email attachment containing malware.

What can I do?

Employees at all levels need to be aware of what their roles and responsibilities are. Train your staff to recognise threats such as phishing emails and other malware or alerting them to the risks involved in posting information relating to your business activities on social networks.

You should encourage general security awareness within your organisation. A security aware culture is likely to identify security risks.

You should also keep your knowledge of threats up-to-date by reading security bulletins or newsletters from organisations relevant to your business.

Keep an eye out for problems

7

What is the problem?

Cyber criminals or malware can attack your systems and go unnoticed for a long time. Many people only find out they have been attacked when it is too late even though the warning signs were there.

What can I do?

Check your security software messages, access control logs and other reporting systems you have in place on a regular basis. You should also act on any alerts that are issued by these monitoring services.

Make sure you can check what software or services are running on your network. Make sure you can identify if there is something there which should not be.

Run regular vulnerability scans and penetration tests to scan your systems for known vulnerabilities – make sure you address any vulnerabilities identified.

8 Know what you should be doing

What is the problem?

A good policy will enable you to make sure you address the risks in a consistent manner. Well written policies should integrate well with business processes.

Some organisations do not have adequate levels of protection because they are not correctly using the security they already have, and are not always able to spot when there is a problem. You should also consider what actions you should put into place should you suffer a data breach. Good incident management can reduce the damage and distress caused to individuals.

What can I do?

Review what personal data you currently have and the means of protection you have in place.

Make sure you are compliant with any industry guidance or other legal requirements.

Document the controls you have in place and identify where you need to make improvements.

Once any improvements are in place, continue to monitor the controls and make adjustments where necessary.

Consider the risks for each type of personal data you hold and how you would manage a data breach. This way you can reduce the impact if the worst was to happen.

You should also have an acceptable-use policy and training materials for staff so that they know their data protection responsibilities.

Minimise your data

9

What is the problem?

The DPA says that personal data should be accurate, up-to-date and kept for no longer than is necessary. Over time you may have collected large amounts of personal data. Some of this data may be out-of-date and inaccurate or no longer useful.

What can I do?

Decide if you still need the data. If you do, make sure it is stored in the right place.

If you have data you need to keep for archive purposes but don't need to access regularly, move it to a more secure location. This will help prevent unauthorised access.

If you have data you really no longer need, you should delete it. This should be in line with your data retention and disposal policies. You might need specialist software or assistance to do this securely.

10 Make sure your IT contractor is doing what they should be

What is the problem?

Many small businesses outsource some or all of their IT requirements to a third party. You should be satisfied that they are treating your data with at least the same level of security as you would.

What can I do?

Ask for a security audit of the systems containing your data. This may help to identify vulnerabilities which need to be addressed.

Review copies of the security assessments of your IT provider.

If appropriate, visit the premises of your IT provider to make sure they are as you would expect.

Check the contracts you have in place. They must be in writing and must require your contractor to act only on your instructions and comply with certain obligations of the DPA

Don’t overlook asset disposal – if you use a contractor to erase data and dispose of or recycle your IT equipment, make sure they do it adequately. You may be held responsible if personal data gathered by you is extracted from your old IT equipment when it is resold.

Further reading

As illustrated by the range of topics covered in this guide, keeping an IT network safe and secure can be a complex task and does require time, resource and specialist knowledge. However, there are a range of organisations offering advice and guidance appropriate to your business.

Get Safe Online (www.getsafeonline.org)
A joint initiative between the government, law enforcement, leading businesses and the public sector to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet

Cyber Street (www.cyberstreetwise.com)
Cyber Street is a cross-government campaign, funded by the National Cyber Security Programme, and delivered in partnership with the private and voluntary sectors. The campaign is led by the Home Office, working closely with the Department for Business, Innovation and Skills and the Cabinet Office.

Cyber Essentials (www.gov.uk/government/publications/cyber-essentials-scheme-overview)
The Cyber Essentials scheme provides businesses small and large with clarity on good basic cyber security practice. By focusing on basic cyber hygiene, your company will be better protected from the most common cyber threats. Cyber Essentials is mandatory for central government contracts advertised after 1 October 2014 that involve handling personal information and providing certain ICT products and services. It has been developed as part of the UK's National Cyber Security Programme in close consultation with industry.

10 Steps to Cyber Security (https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility)
The 10 Steps define and communicate an Information Risk Management Regime which can provide protection against cyber attacks.

Action Fraud (www.actionfraud.police.uk)
Action Fraud is the UK's national reporting centre for victims of fraud or financially motivated internet crime. Action Fraud records and refers these crimes to the police and provides victims with a crime reference number, support and advice.

If you would like to contact us please call 0303 123 1113

www.ico.org.uk

Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire, SK9 5AF

6 January 2016

Upholding information rights